Windows Hello for Business

Nicola Suter

About

Nicola Suter

Modern Workplace engineer for itnetX (Switzerland) AG

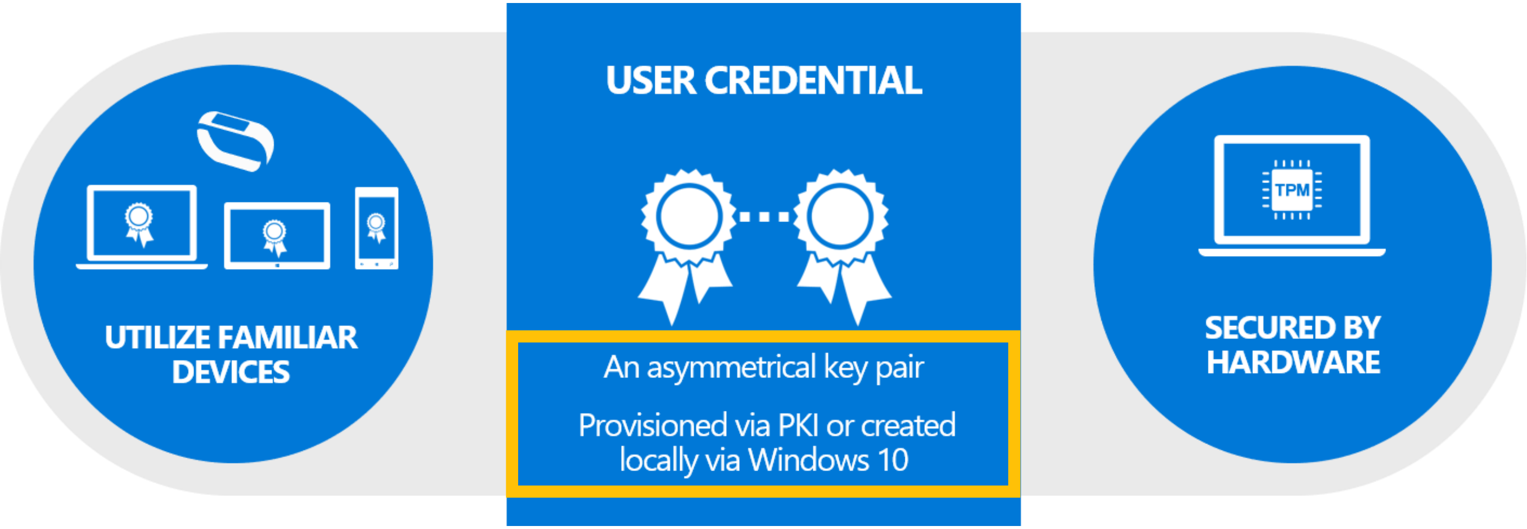
BSc student in computer sciences

Blog: tech.nicolonsky.ch

Twitter: @nicolonsky

Advantages over passwords

- Device based multi factor authentication
- Passwordless



UTILIZE FAMILIAR DEVICES

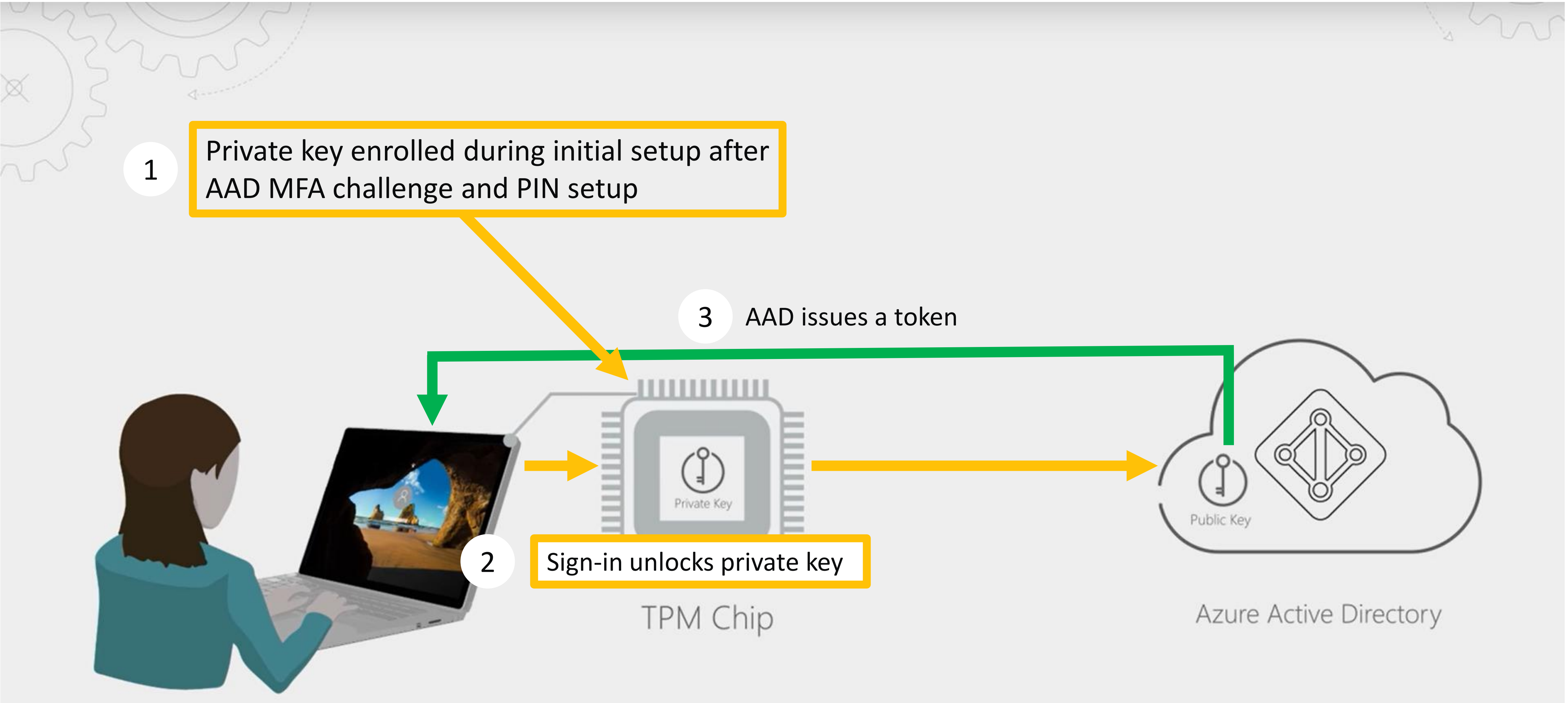
USER CREDENTIAL

An asymmetrical key pair

Provisioned via PKI or created locally via Windows 10

SECURED BY HARDWARE

What is Windows Hello for Business?



1 Private key enrolled during initial setup after AAD MFA challenge and PIN setup

2 Sign-in unlocks private key

3 AAD issues a token

Deployment scenarios

Device state	User state	Effort
Azure AD Joined	**Azure AD user**	**-**
Azure AD Joined	**Hybrid identity**	**++, +++**
Hybrid Azure AD Joined	**Hybrid identity**	**+, ++**
Domain Joined	AD user	++++

Prerequisites

- Windows 10 1903 (introduced FIDO2 key sign-in)
- Azure Active Directory

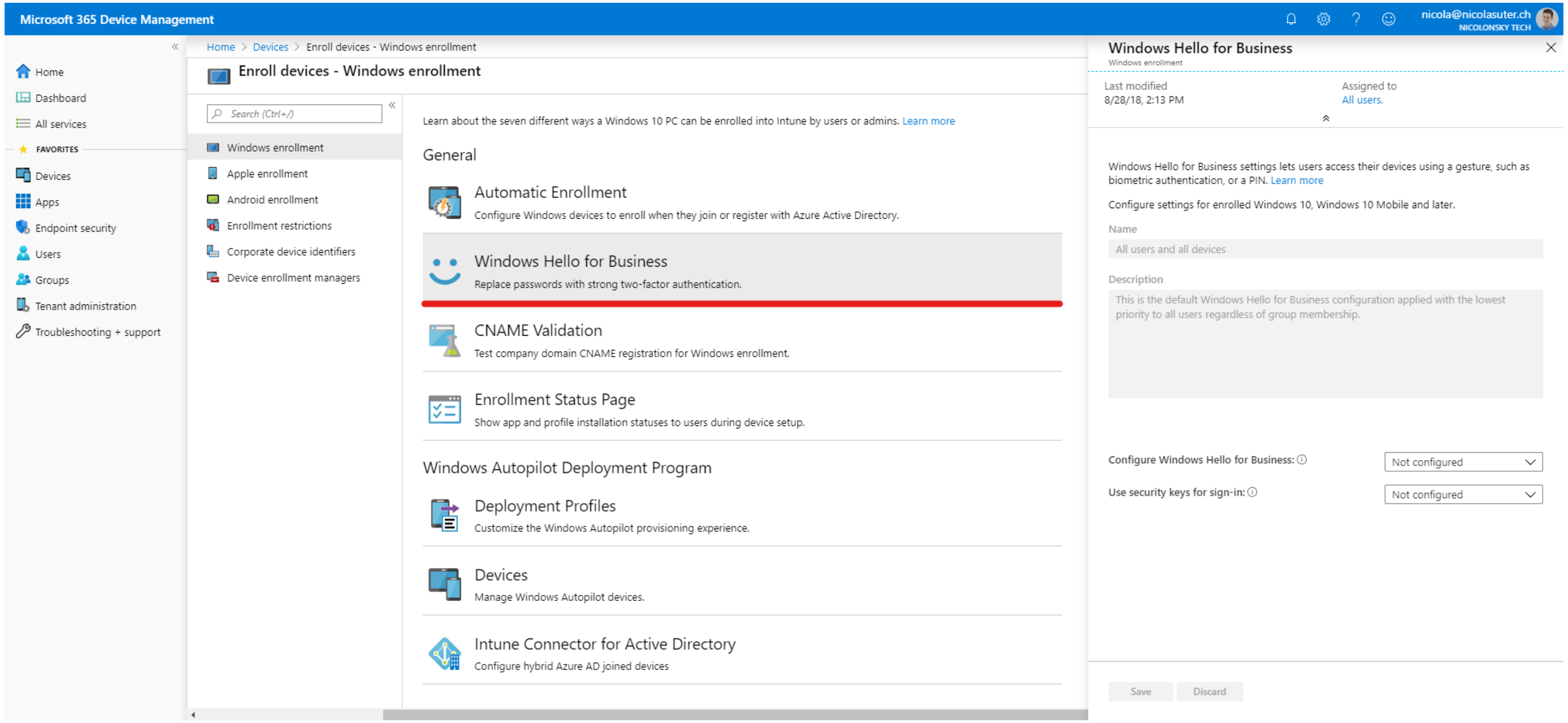
Recommended prerequisites:

- TPM (if no TPM present, private key gets enrolled to software KSP → less secure)
- Hardware with biometric support (IR camera, fingerprint)

Management tools

Windows Hello for Business settings can be managed with:

- Group Policy
- Microsoft Intune (passportforwork-csp)
- Microsoft Endpoint Configuration Manager; deprecated



Enroll devices - Windows enrollment

Learn about the seven different ways a Windows 10 PC can be enrolled into Intune by users or admins. Learn more

General

Automatic Enrollment
Configure Windows devices to enroll when they join or register with Azure Active Directory.

Windows Hello for Business
Replace passwords with strong two-factor authentication.

CNAME Validation
Test company domain CNAME registration for Windows enrollment.

Enrollment Status Page
Show app and profile installation statuses to users during device setup.

Windows Autopilot Deployment Program

Deployment Profiles
Customize the Windows Autopilot provisioning experience.

Devices
Manage Windows Autopilot devices.

Intune Connector for Active Directory
Configure hybrid Azure AD joined devices

Windows Hello for Business
Windows enrollment

Last modified: 8/28/18, 2:13 PM
Assigned to: All users.

Windows Hello for Business settings lets users access their devices using a gesture, such as biometric authentication, or a PIN. Learn more

Configure settings for enrolled Windows 10, Windows 10 Mobile and later.

Name: All users and all devices

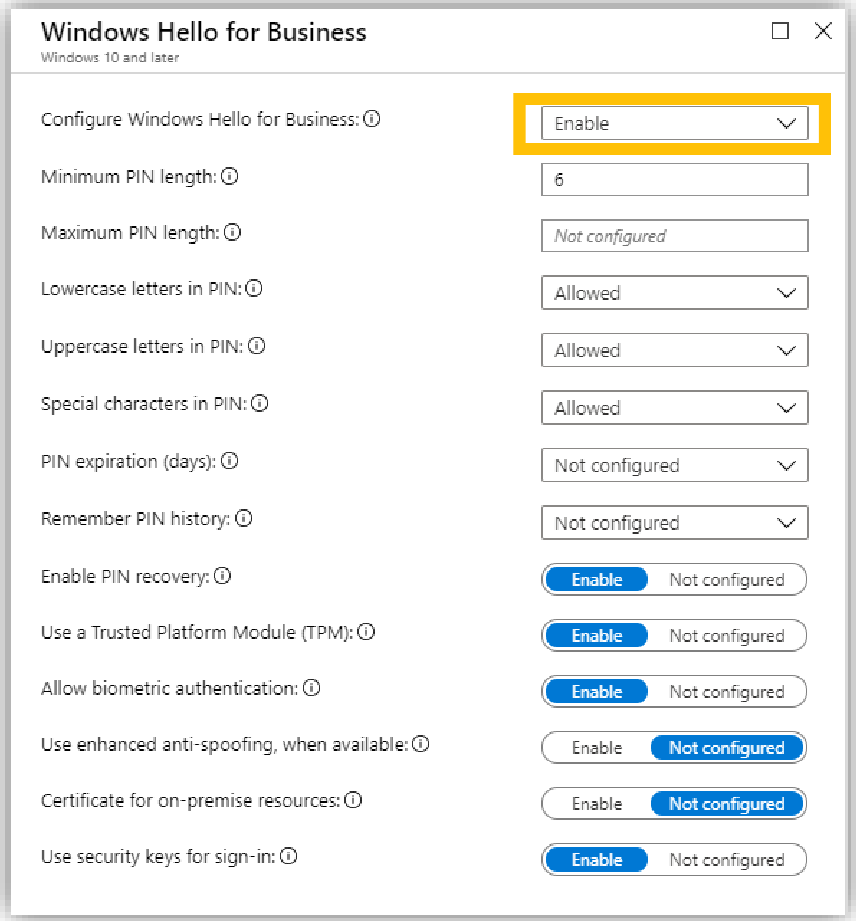
Description: This is the default Windows Hello for Business configuration applied with the lowest priority to all users regardless of group membership.

Configure Windows Hello for Business: Not configured

Use security keys for sign-in: Not configured

Management tools - Intune

- Dedicated profile type: "identity protection"
- Overrides configured settings in device enrollment!



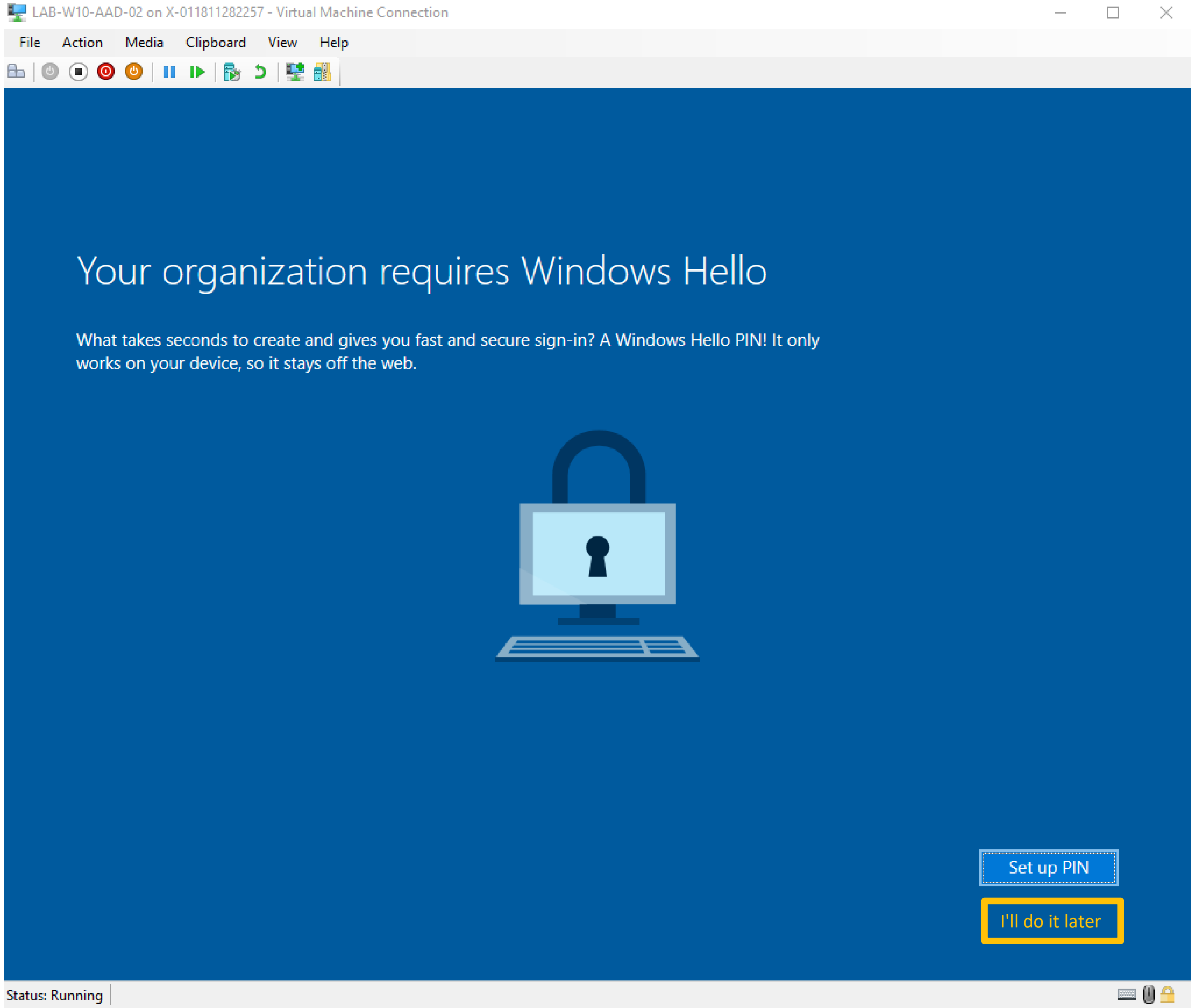
Windows Hello for Business

Windows 10 and later

Configure Windows Hello for Business: ⓘ	Enable
Minimum PIN length: ⓘ	6
Maximum PIN length: ⓘ	*Not configured*
Lowercase letters in PIN: ⓘ	Allowed
Uppercase letters in PIN: ⓘ	Allowed
Special characters in PIN: ⓘ	Allowed
PIN expiration (days): ⓘ	Not configured
Remember PIN history: ⓘ	Not configured
Enable PIN recovery: ⓘ	[✓ Enable] Not configured
Use a Trusted Platform Module (TPM): ⓘ	[✓ Enable] Not configured
Allow biometric authentication: ⓘ	[✓ Enable] Not configured
Use enhanced anti-spoofing, when available: ⓘ	Enable [✓ Not configured]
Certificate for on-premise resources: ⓘ	Enable [✓ Not configured]
Use security keys for sign-in: ⓘ	[✓ Enable] Not configured

geekmania 2019 switzerland

End user experience



LAB-W10-AAD-02 on X-011811282257 - Virtual Machine Connection
File
Action
Media
Clipboard
View
Help

Your organization requires Windows Hello

What takes seconds to create and gives you fast and secure sign-in? A Windows Hello PIN! It only works on your device, so it stays off the web.

Multifactor unlock

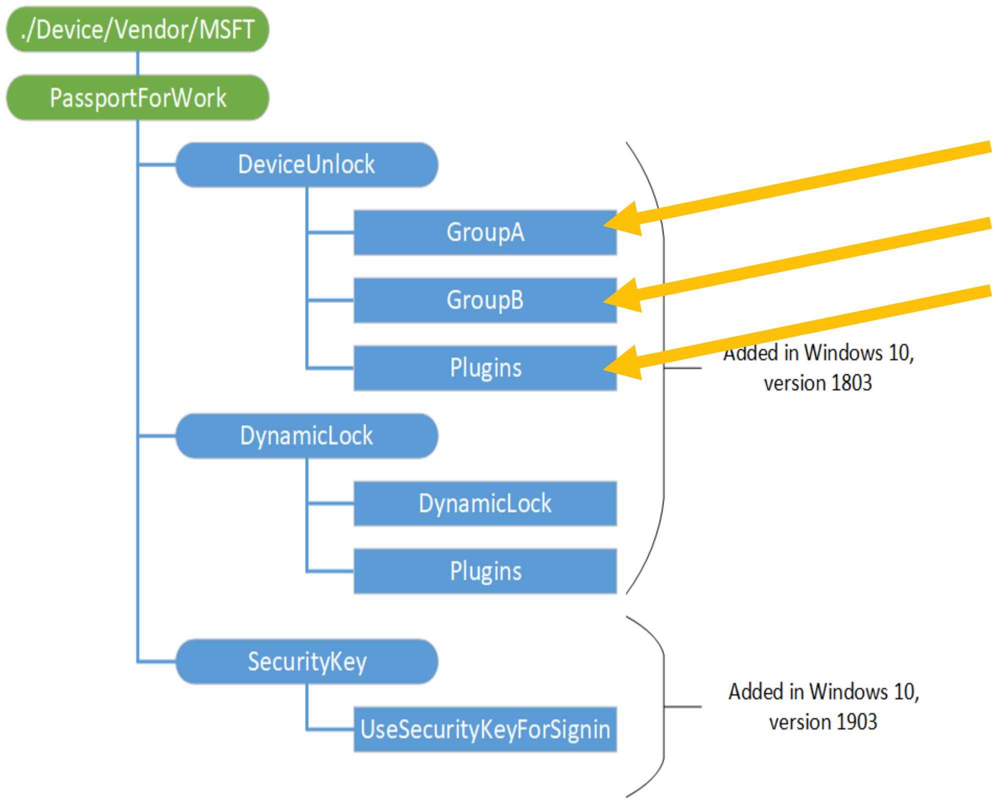
- Require an additional factor to unlock a device
- Benefit as long as password sign-ins are still possible?

First unlock factor	Second unlock factor
•PIN •Fingerprint •Facial Recognition	• PIN • Trusted Signal • Phone proximity • Network location • Wi-Fi network

a credential supported by that provider can **only satisfy one** of the unlock factors

Multifactor unlock – config and demo

Configuration with Intune policy CSP:



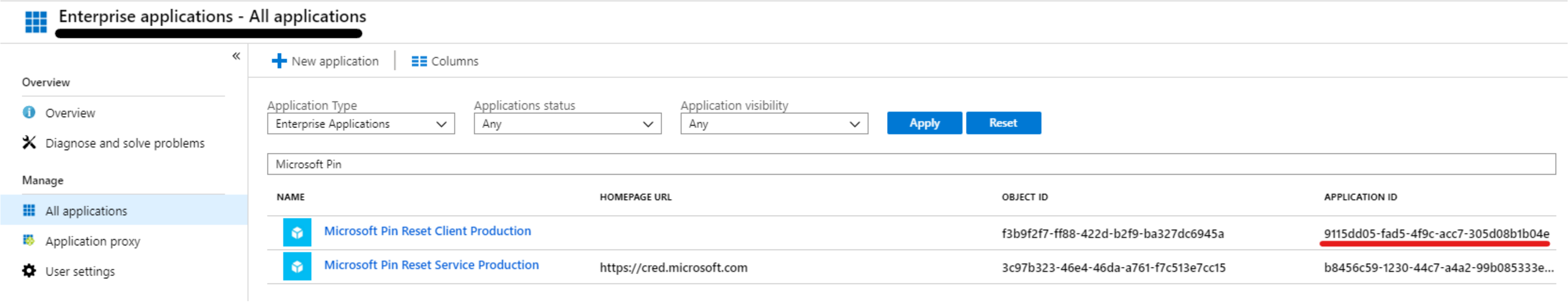
First unlock factor

Second unlock factor

Trusted signals

PIN reset

- Reset WHFB PIN from lock screen or ms-settings app
- Admin consent for Azure AD applications required!



Enterprise applications - All applications

[redacted]

Application Type: Enterprise Applications

Applications status: Any

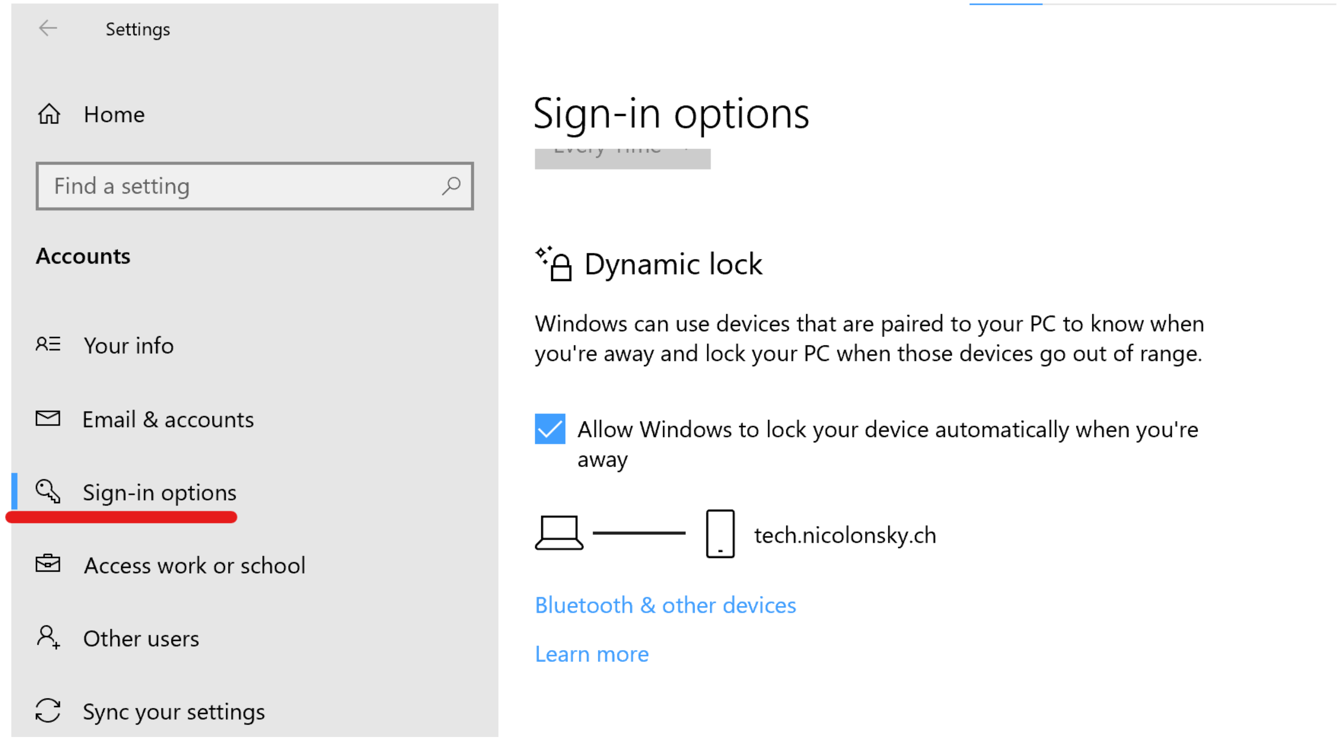
Application visibility: Any

Microsoft Pin

NAME	HOMEPAGE URL	OBJECT ID	APPLICATION ID
Microsoft Pin Reset Client Production		f3b9f2f7-ff88-422d-b2f9-ba327dc6945a	9115dd05-fad5-4f9c-acc7-305d08b1b04e
Microsoft Pin Reset Service Production	https://cred.microsoft.com	3c97b323-46e4-46da-a761-f7c513e7cc15	b8456c59-1230-44c7-a4a2-99b085333e...

Dynamic lock

- Automatically lock device screen when paired device moves
- Improves default value of 15 minutes for the screen lock
- Uses Bluetooth Received Signal Strength Indication (RSSI)
- Required signal strength can be overridden



Sign-in options

Dynamic lock

Windows can use devices that are paired to your PC to know when you're away and lock your PC when those devices go out of range.

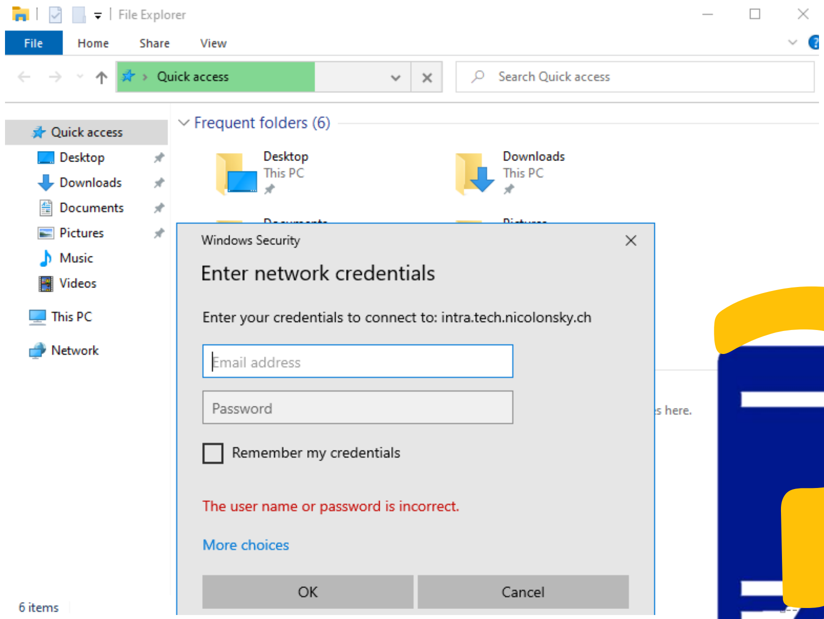
☑ Allow Windows to lock your device automatically when you're away

tech.nicolonsky.ch

Bluetooth & other devices

Learn more

On premise resource access



Windows Security

Enter network credentials

Enter your credentials to connect to: intra.tech.nicolonsky.ch

Email address

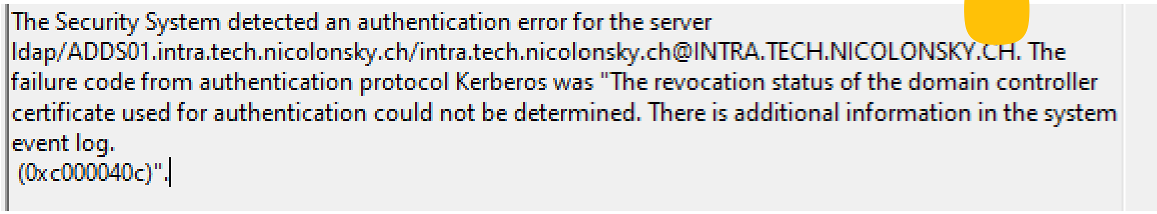
Password

□ Remember my credentials

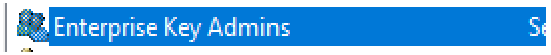
The user name or password is incorrect.

More choices

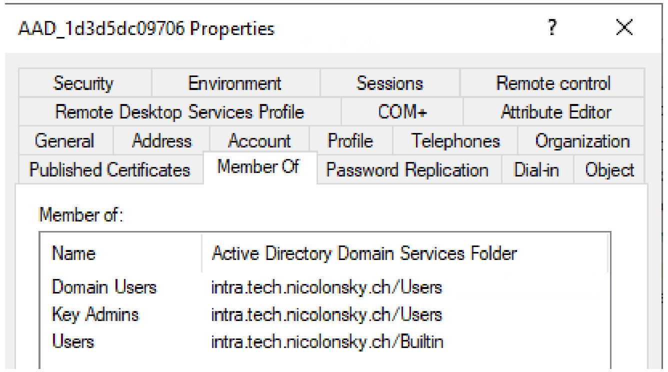
OK Cancel



The Security System detected an authentication error for the server ldap/ADDS01.intra.tech.nicolonsky.ch/intra.tech.nicolonsky.ch@INTRA.TECH.NICOLONSKY.CH. The failure code from authentication protocol Kerberos was "The revocation status of the domain controller certificate used for authentication could not be determined. There is additional information in the system event log.
(0xc000040c)".



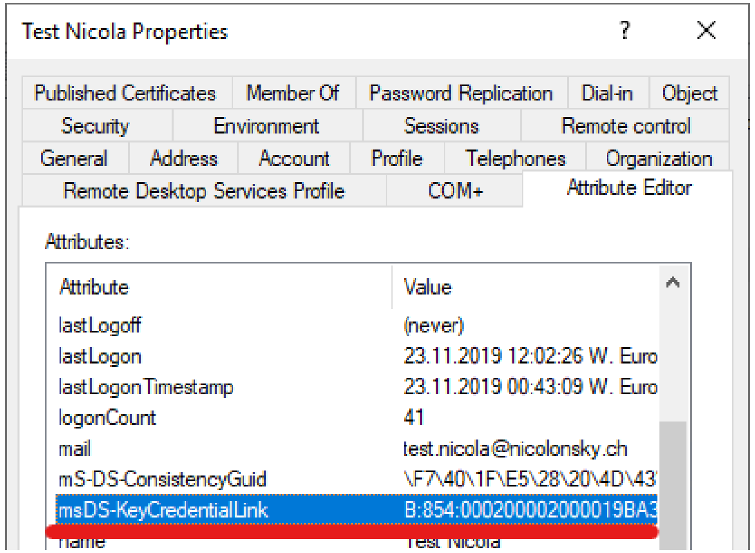
Enterprise Key Admins Se



AAD_1d3d5dc09706 Properties ? ×

Member of:

Name	Active Directory Domain Services Folder
Domain Users	intra.tech.nicolonsky.ch/Users
Key Admins	intra.tech.nicolonsky.ch/Users
Users	intra.tech.nicolonsky.ch/Builtin



Test Nicola Properties ? ×

Attributes:

Attribute	Value
lastLogoff	(never)
lastLogon	23.11.2019 12:02:26 W. Euro
lastLogonTimestamp	23.11.2019 00:43:09 W. Euro
logonCount	41
mail	test.nicola@nicolonsky.ch
mS-DS-ConsistencyGuid	\F7\40\1F\E5\28\20\4D\43
msDS-KeyCredentialLink	B:854:000200002000019BA3
name	Test Nicola

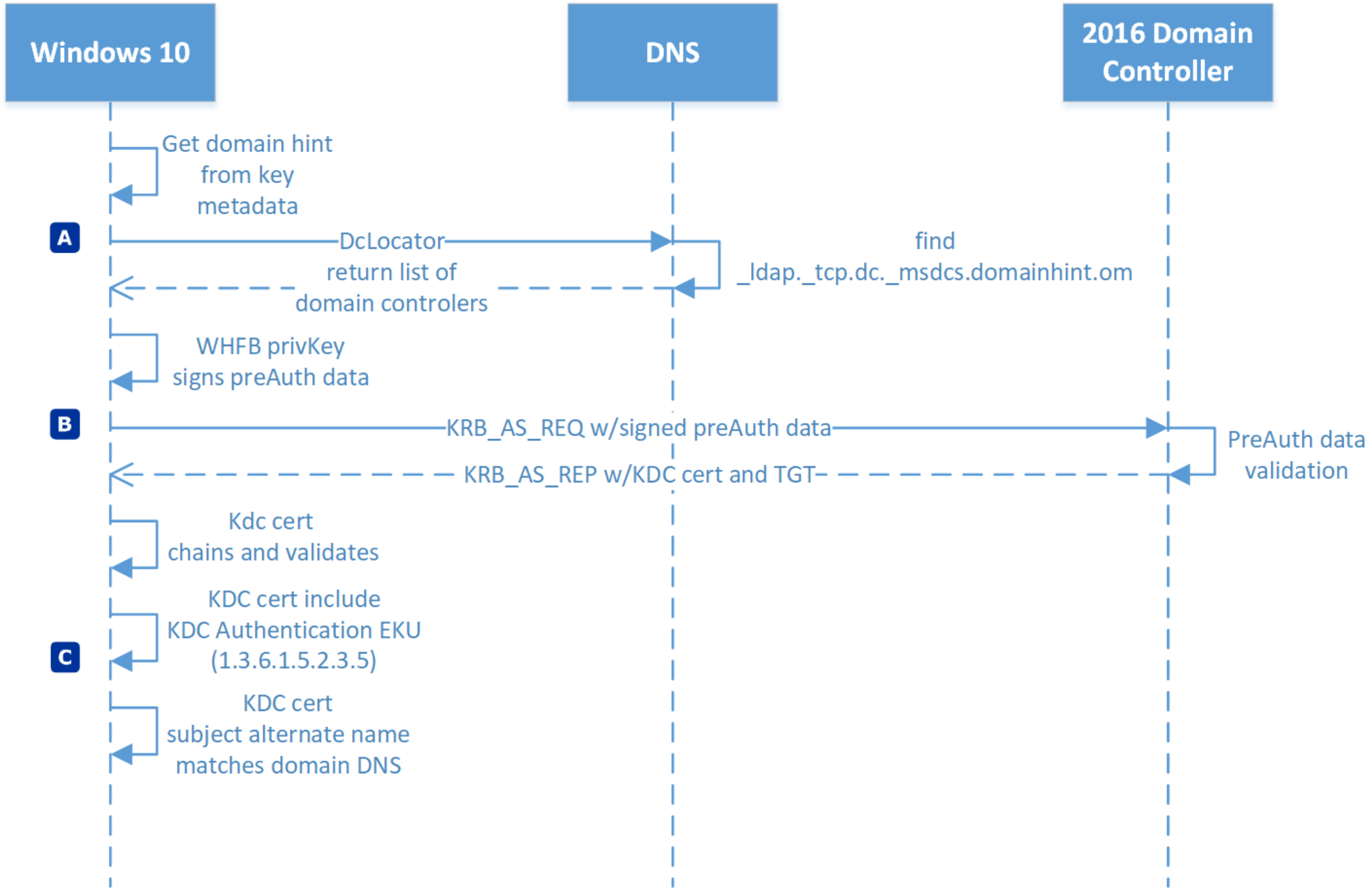
AAD Join deployment options

	Key based authentication	Certificate based authentication
Prerequisites	•At least one Server 2016 DC •Server 2012 Enterprise CA •Azure AD Connect	•Windows Server 2008R2 DC'S •Server 2012 Enterprise CA •Azure AD Connect •Azure AD App Proxy •NDES Server
Choose when	•Running 2016 DC's •Want to invest a minimal effort	•Already running NDES •Use other certificates with NDES
Microsoft docs	•aadj-sso-base	•aadj-sso-cert

Hybrid AAD Join deployment options

	Key based authentication	Certificate based authentication
Prerequisites	•At least one Server 2016 DC •Server 2012 Enterprise CA •Azure AD Connect	•Windows Server 2008R2 DC'S •Server 2012 Enterprise CA •Server 2016 ADFS •Device Synchronisation •Device writeback
Choose when	•Running 2016 DC's •Want to invest a minimal effort	•You love complex legacy set-ups
Microsoft docs	•hello-hybrid-key-trust	•hello-hybrid-cert-trust

AAD Join and AD authentication



Windows 10

DNS

2016 Domain Controller

Get domain hint from key metadata

A

DcLocator

find _ldap._tcp.dc._msdcs.domainhint.om

return list of domain controlers

WHFB privKey signs preAuth data

B

KRB_AS_REQ w/signed preAuth data

PreAuth data validation

KRB_AS_REP w/KDC cert and TGT

Kdc cert chains and validates

C

KDC cert include KDC Authentication EKU (1.3.6.1.5.2.3.5)

KDC cert subject alternate name matches domain DNS

Notes from the field

- AAD Connect Service Account must be in the Key Admin group
- AAD Connect member of key admin group (msDs-KeyCredentialslLink)
- Refresh directory scheme on AAD Connect after AD scheme extension
- CRL, CRL, CRL → test it with certutil
  - Must be accessible from any Windows 10 WHFB client
- Use "Kerberos Authentication" template to enroll on DC's
  - Verify that domain name is addedd to the SAN
  - Check KDC in certification usage!
  - Verify key size (2048)

Hybrid Azure AD Joined devices:

- SCP entry in AD

Making Windows 10 passwordless?

Remove password surface:

- Disable password sign-in by policy
- Hide password sign-in credential provider from lock screen

As alternative use:

- Web-Sign-In from Lock-Screen for intial passwordless sign-in's on existing devices

Passwordless Azure AD Join and Intune enrollment:

- Authenticator with phone sign-in (needs to be preconfigured)

Recap

- Go for a WHFB deployment
- Configure SSO for on premise resource access
- Purchase devices with WHFB capabilities

Gold-Sponsor:

itrain

THE ESSENCE OF IT

Silver-Sponsor:

baseVISION

SECURE & MODERN WORKPLACE

Thank You

geekmania 2019

switzerland